Cisco Unity Connection 用 Cisco Unified Communications Operating System アドミニストレーションガイド

リリース 11.x
2015 年 5 月発行

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices.

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Unified Communications Operating System アドミニストレーション ガイド for Cisco Unity Connection リリース 11.x

はじめに 5
対象読者および使用 5
表記法 5
関連資料 7
Cisco Business Edition に関するマニュアル リファレンス 7
マニュアルの入手方法およびテクニカル サポート 7
シスコ製品のセキュリティ 7

CHAPTER 1 はじめに 1-1
概要 1-1
ブラウザ要件 1-2
オペレーティング システムのステータスと設定 1-2
設定 1-3
セキュリティ設定 1-3
ソフトウェアのアップグレード 1-4
コマンドライン インターフェイス 1-4

CHAPTER 2 Cisco Unified Communications Operating System の管理へのログイン 2-1
Cisco Unified Communications Operating System の管理へのログイン 2-1
OS 管理者パスワードとセキュリティ パスワードのリセット 2-2

CHAPTER 3 ステータスと設定 3-1
クラスタ ノード 3-1
ハードウェア ステータス 3-2
ネットワークの設定 3-2
インストールされているソフトウェア 3-4
システム ステータス 3-4
IP プリファレンス 3-5

CHAPTER 4 設定 4-1
IP 設定 4-1
イーサネット設定 4-1
イーサネット IPv6 の設定 4-2
パブリッシャ設定 4-3
NTP サーバ 4-4
SMTP 設定 4-5
時間設定 4-5

CHAPTER 5 システム リスタート 5-1
バージョンの切り替えと再起動 5-1
現在のバージョンの再起動 5-2
システムのシャットダウン 5-2

CHAPTER 6 セキュリティ 6-1
Internet Explorer のセキュリティ オプションの設定 6-1
証明書と証明書信頼リストの管理 6-1
証明書の表示 6-2
証明書のダウンロード 6-2
証明書の削除と再作成 6-3
証明書の削除 6-3
証明書の再生成 6-3
サードパーティ製の CA 証明書の使用 6-4
シングルサーバとマルチサーバの証明書の概要 6-4
証明書署名要求の生成 6-6
証明書署名要求のダウンロード 6-7
サードパーティ製の CA 証明書 6-8
信頼証明書のアップロード 6-8
アプリケーション証明書のアップロード 6-9
証明書の有効期限日のモニタ 6-9
証明書の失効 6-10
オンライン証明書ステータス プロトコルの設定 6-10
IPSEC の管理 6-11
新しい IPSec ポリシーの設定 6-11
既存の IPSec ポリシーの管理 6-13

CHAPTER 7 ソフトウェアのアップグレード 7-1
カスタム ログイン メッセージの設定 7-1

CHAPTER 8 サービス 8-1
ping 8-1
リモート サポート 8-2
INDEX

はじめに

ここでは、次の項について説明します。

- 対象読者および使用（5 ページ）
- 表記法（5 ページ）
- 関連資料（7 ページ）
- Cisco Business Edition に関するマニュアル リファレンス（7 ページ）
- シスコ製品のセキュリティ（7 ページ）

対象読者および使用

『*Cisco Unified Communications Operating System Administration Guide*』は、Cisco Unified Communications Operating System のグラフィカル ユーザ インターフェイス（GUI）の使用に関する情報を提供します。

このマニュアルは、Cisco Unified Communications Operating System の管理およびサポートを担当するネットワーク管理者を対象としています。ネットワーク エンジニア、システム管理者、またはテレコム エンジニアはこのマニュアルを使用して、オペレーティング システムの機能を学習し管理します。このマニュアルを使用するには、テレフォニーおよび IP ネットワーキング テクノロジーに関する知識が必要です。

さまざまなシステムおよびネットワークに関連する共通タスクを実行する際に使用できるコマンドライン インターフェイス（CLI）の詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字フォント	コマンドおよびキーワードは**太字**で示しています。
italic フォント	ユーザが値を指定する引数は、*イタリック体*で表記されています。
[ ]	角カッコの中の要素は、省略可能です。

表記法	説明
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、**太字の `screen` フォント**で示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、*イタリック体の screen* フォントで示しています。
	このポインタは、例の中の重要な行を強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。

『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』では、次の表記法も使用します。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント アドバイス 「*時間の節約に役立つ操作*」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒント *役立つ「ヒント」*の意味です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 **この警告マークは、危険な状態を警告するものです。傷害を負う可能性がある状況です。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。**

関連資料

関連する Cisco IP テレフォニーのアプリケーションおよび製品の詳細については、次の URL にある該当するリリース番号の『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

Cisco Business Edition に関するマニュアル リファレンス

Cisco Unity Connection 11.x マニュアル セットでは、「Cisco Business Edition」と Cisco Unified CMBE への参照は Business Edition 6000/7000 に適用されます。参照はその他の Business Edition には適用されません。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は Really Simple Syndication（RSS）フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、次の URL で参照できます。
http://www.access.gpo.gov/bis/ear/ear_data.html

はじめに

Cisco Unified Communications Manager と Cisco Unity Connection では、Cisco Unified Communications Operating System を使用して多くの一般的なシステム管理機能を実行できます。

この章は、次の項で構成されています。

- 概要（1-1 ページ）
- ブラウザ要件（1-2 ページ）
- オペレーティング システムのステータスと設定（1-2 ページ）
- 設定（1-3 ページ）
- セキュリティ設定（1-3 ページ）
- ソフトウェアのアップグレード（1-4 ページ）
- このアプリケーションでは、次のオペレーティング システム ユーティリティを使用できます。（1-4 ページ）
- コマンドライン インターフェイス（1-4 ページ）

概要

Cisco Unified Communications Operating Systemの管理では、Cisco Unified Communications Operating Systemの設定と管理ができます。管理タスクの例として、次のようなものがあげられます。

- ソフトウェアとハードウェアのステータスを確認する。
- IP アドレスの確認と更新を行う。
- 他のネットワーク デバイスに ping を送信する。
- NTP サーバを管理する。
- システム ソフトウェアおよびオプションをアップグレードする。
- サーバをセキュリティ管理する（IPSec や証明書なども含む）。
- リモート サポート アカウントを管理する。
- システムを再起動する。

次の各項では、オペレーティング システムの各機能の詳細について説明します。

ブラウザ要件

Cisco Unified Communications Operating System にアクセスするには、次のブラウザが必要です。

Cisco Unified Communications Operating Systemへのアクセスに使用するブラウザ	使用するオペレーティング システム
Microsoft Internet Explorer 8	• Microsoft XP service pack 3 • Microsoft Vista service pack 2 以降のサービス パック • 最新のサービス パックをインストールした Microsoft Windows 7
Mozilla Firefox 3.x	• Microsoft XP service pack 3 • Microsoft Vista service pack 2 以降のサービス パック • 最新のサービス パックをインストールした Microsoft Windows 7 • 最新のサービス パックをインストールした Apple MAC OS X
Safari 4.x	Apple MAC OS X

製品のすべての機能が正常に動作するには、ブラウザの「信頼済みサイト ゾーン」や「ローカル イントラネット サイト ゾーン」に Cisco Unified Communications Operating System サーバの URL（**https://***servername*）が含まれている必要があります。

オペレーティング システムのステータスと設定

[表示（Show）] メニューから、オペレーティング システムの次のような各種のコンポーネントのステータスを確認できます。

- クラスタおよびノード
- ハードウェア
- ネットワーク
- システム
- インストールされているソフトウェアとオプション

詳細については、「ステータスと設定」の章を参照してください。

設定

[設定(Settings)] メニューから、オペレーティング システムに関する次の設定の表示と更新ができます。

- [IP]:アプリケーションのインストール時に入力された IP アドレスおよび Dynamic Host Configuration Protocol(DHCP)クライアントの設定を更新します。
- [NTPサーバの設定(NTP Server Settings)]:外部 NTP サーバの IP アドレスの設定、および NTP サーバの追加と削除を行います。
- [SMTP設定(SMTP settings)]:オペレーティング システムが電子メール通知の送信に使用する SMTP ホストを設定します。

詳細については、「設定」の章を参照してください。

[設定(Settings)] > [バージョン(Version)] ウィンドウでは、システムの再起動やシャットダウンに関する次のオプションを選択できます。

- [バージョンの切り替え(Switch Versions)]:アクティブなディスク パーティションと非アクティブなディスク パーティションを切り替えて、システムを再起動します。通常、このオプションを選択するのは、非アクティブなパーティションを更新した後で、かつ新しいバージョンのソフトウェアの実行を開始する場合です。
- [現在のバージョン(Current Version)]:パーティションを切り替えずにシステムを再起動します。
- [システムのシャットダウン(Shutdown System)]:実行中のソフトウェアをすべて停止し、サーバをシャットダウンします。

(注) このコマンドではサーバの電源は切断されません。サーバの電源を切断するには、電源ボタンを押します。

詳細については、「システム リスタート」の章を参照してください。

セキュリティ設定

オペレーティング システムのセキュリティ オプションを使用すると、セキュリティ証明書と Secure Internet Protocol(IPSec)を管理できます。[セキュリティ(Security)] メニューでは、次のセキュリティ オプションを選択できます。

- [証明書の管理(Certificate Management)]:証明書、証明書信頼リスト(CTL)、および証明書署名要求(CSR)を管理します。証明書の表示、アップロード、ダウンロード、削除、および再作成を行うことができます。[証明書の管理(Certificate Management)] を使用すると、サーバ上の証明書の有効期限をモニタすることもできます。
- [IPSECの管理(IPSEC Management)]:既存の IPSEC ポリシーの表示または更新、新規の IPSEC ポリシーとアソシエーション設定を行います。

詳細については、「セキュリティ」の章を参照してください。

ソフトウェアのアップグレード

ソフトウェア アップグレード オプションを使用すると、オペレーティング システムで実行されているソフトウェア バージョンをアップグレードしたり、特定のソフトウェア オプション（Cisco Unified Communications Operating System ロケール インストーラ、ダイヤル プラン、TFTP サーバ ファイルなど）をインストールしたりできます。

[インストール/アップグレード（Install/Upgrade）] メニュー オプションで、ローカル ディスクまたはリモート サーバからシステム ソフトウェアをアップグレードできます。アップグレードしたソフトウェアは非アクティブなパーティションにインストールされ、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムで新しいソフトウェア バージョンが実行されます。

（注）　Cisco Unified Communications Operating System GUI およびコマンドライン インターフェイスに含まれるソフトウェア アップグレード機能を使用して、すべてのソフトウェアのインストールとアップグレードを実行する必要があります。このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。Cisco Unified Communications Manager の以前のバージョンで使用していたサードパーティ製もしくは Windows ベースのソフトウェア アプリケーションは、インストールしたり使用したりできません。

詳細については、「ソフトウェアのアップグレード」の章を参照してください。

このアプリケーションでは、次のオペレーティング システム ユーティリティを使用できます。

- **ping**：他のネットワーク デバイスとの接続を確認します。
- **リモート サポート**：シスコのサポート担当者がシステムへのアクセスに使用できるアカウントを設定します。このアカウントは、指定した日数が経過すると自動的に失効します。

詳細については、「サービス」の章を参照してください。

コマンドライン インターフェイス

コマンドライン インターフェイスにアクセスするには、コンソールを使用するか、サーバにセキュア シェル接続します。詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

CHAPTER 2

Cisco Unified Communications Operating System の管理へのログイン

この章では、Cisco Unified Communications Operating Systemの管理にアクセスする手順および紛失したパスワードを回復する手順について説明します。

この章は、次の項で構成されています。

- Cisco Unified Communications Operating Systemの管理へのログイン（2-1 ページ）
- OS 管理者パスワードとセキュリティ パスワードのリセット（2-2 ページ）

Cisco Unified Communications Operating Systemの管理へのログイン

Cisco Unified Communications Operating Systemの管理にアクセスしてログインするには、次の手順に従います。

（注） Cisco Unified Communications Operating System の管理を使用する場合、ブラウザのコントロール（[戻る（Back）] ボタンなど）は使用しないでください。

手順

ステップ 1 Cisco Unity Connection Administration の URL を参照します。

ステップ 2 Cisco Unity Connection Administration ウィンドウの右上にある [ナビゲーション（Navigation）] メニューで [Cisco Unified OSの管理（Cisco Unified OS Administration）] を選択し、[移動（Go）] をクリックします。

[Cisco Unified Communications オペレーティング システムの管理へのログイン（Cisco Unified Communications Operating System Administration Logon）] ウィンドウが表示されます。

（注） また、次の URL を入力して[Cisco Unified Communications Operating Systemの管理（Cisco Unified Operating System Administration）] に直接アクセスすることもできます。
http://*server-name***/cmplatform**

ステップ 3　管理者ユーザ名とパスワードを入力します。

（注）　管理者ユーザ名とパスワードは、インストール時に決めるか、コマンド ライン インターフェイスを使用して作成します。

ステップ 4　[送信（Submit）] をクリックします。

[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウが表示されます。

OS 管理者パスワードとセキュリティ パスワードのリセット

管理者パスワードやセキュリティ パスワードがわからなくなった場合、次の手順に従ってパスワードをリセットします。

パスワードをリセットするには、システム コンソール経由でシステムに接続している必要があります。つまり、キーボードとモニタをサーバに接続している必要があります。システムにセキュア シェル接続している状態ではパスワードをリセットできません。

注意　セキュリティ パスワードは、クラスタ内のすべてのノードで一致している必要があります。セキュリティ パスワードは、すべてのマシン上で変更してください。変更していない場合、クラスタ ノードが通信不能になります。

注意　セキュリティ パスワードを変更した後に、クラスタ内の各サーバをリセットする必要があります。サーバ（ノード）をリブートしない場合、システム サービスで問題が発生するほか、サブスクライバ サーバ上の Cisco Unified Communications Manager Administration ウィンドウで問題が発生します。

（注）　この手順中、物理的にシステムにアクセスできることを確認するために、有効な CD または DVD をディスク ドライブから取り出し、再挿入する必要があります。

手順

ステップ 1　次のユーザ名とパスワードを使用してシステムにログインします。

- ユーザ名：**pwrecovery**
- パスワード：**pwreset**

[プラットフォーム パスワードのリセットへようこそ（Welcome to platform password reset）] ウィンドウが表示されます。

ステップ 2　何かキーを押して続行します。

ステップ 3　ディスク ドライブに CD または DVD が入っている場合は、ここで取り出します。

ステップ 4　何かキーを押して続行します。

CD または DVD をディスク ドライブから取り出してあるかが確認されます。

ステップ 5　有効な CD または DVD をディスク ドライブに挿入します。

（注）　このテストでは、音楽 CD ではなくデータ CD を使用する必要があります。

ディスクを挿入したかが確認されます。

ステップ 6　ディスクが挿入されていることが確認されると、次のいずれかのオプションを入力して続行するように指示されます。

- 管理者パスワードをリセットする場合は、**a** を入力します。
- セキュリティ パスワードをリセットする場合は、**s** を入力します。
- 終了する場合は、**q** を入力します。

ステップ 7　作成したタイプの新しいパスワードを入力します。

ステップ 8　新しいパスワードを再入力します。

パスワードには 6 文字以上が必要です。新しいパスワードの強度がチェックされます。パスワードが強度テストにパスしない場合、新しいパスワードを入力するように指示されます。

ステップ 9　新しいパスワードの強度が検証されると、パスワードがリセットされ、任意のキーを押してパスワード リセット ユーティリティを終了するように指示されます。

CHAPTER 3

ステータスと設定

この章ではシステムの管理について説明します。この章は次の内容で構成されています。

- クラスタ ノード（3-1 ページ）
- ハードウェア ステータス（3-2 ページ）
- ネットワークの設定（3-2 ページ）
- インストールされているソフトウェア（3-4 ページ）
- システム ステータス（3-4 ページ）
- IP プリファレンス（3-5 ページ）

クラスタ ノード

クラスタ内の各ノードの情報を表示するには、次の手順に従います。

手順

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで [表示（Show）] > [クラスタ（Cluster）] の順に移動します。

[クラスタ ノード（Cluster Nodes）] ウィンドウが表示されます。

ステップ 2 [クラスタ ノード（Cluster Nodes）] ウィンドウの各フィールドについては、表 3-1を参照してください。

表 3-1　[クラスタノード（Cluster Nodes）] フィールドの説明

フィールド	説明
ホストネーム	サーバの完全なホスト名が表示されます。
[IPアドレス（IP Address）]	サーバの IP アドレスが表示されます。
[エイリアス（Alias）]	サーバのエイリアス名が設定されている場合は、そのエイリアス名が表示されます。
ノードのタイプ（Type of Node）	サーバがパブリッシャ ノードであるかサブスクライバ ノードであるかを表します。

ハードウェア ステータス

ハードウェアのステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウから [表示（Show）] > [ハードウェア（Hardware）] の順に移動します。

[ハードウェアステータス（Hardware Status）] ウィンドウが表示されます。

ステップ 2　[ハードウェアステータス（Hardware Status）] ウィンドウの各フィールドについては、表 3-2 を参照してください。

表 3-2　[ハードウェア ステータス（Hardware Status）] のフィールドの説明

フィールド	説明
プラットフォーム タイプ（Platform Type）	プラットフォーム サーバのモデル ID が表示されます。
プロセッサ速度（Processor Speed）	プロセッサの速度が表示されます。
CPU タイプ（CPU Type）	プラットフォーム サーバのプロセッサのタイプが表示されます。
メモリ	メモリの合計量が MB 単位で表示されます。
オブジェクト ID（Object ID）	オブジェクト ID が表示されます。
OS のバージョン	オペレーティング システムのバージョンが表示されます。
RAIDの詳細（RAID Details）	RAID ドライブの詳細（コントローラの情報、論理ドライブの情報、物理デバイスの情報など）が表示されます。

ネットワークの設定

表示されるネットワーク ステータス情報は、[ネットワーク耐障害性（Network Fault Tolerance）] が有効になっているかどうかによって異なります。[ネットワーク耐障害性（Network Fault Tolerance）] が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を継承します。ネットワーク耐障害性が有効になっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。ネットワーク耐障害性が有効になっていない場合、イーサネット 0 のステータス情報のみが表示されます。

ネットワークのステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウから [表示（Show）] > [ネットワーク（Network）] の順に移動します。

[ネットワーク設定(Network Settings)] ウィンドウが表示されます。

ステップ 2　[ネットワーク設定(Network Settings)] ウィンドウの各フィールドについては、表 3-3を参照してください。

表 3-3　[ネットワークの設定(Network Configuration)] フィールドの説明

フィールド	[説明(Description)]
イーサネットの詳細(Ethernet Details)	
DHCP	イーサネット ポート 0 に対して DHCP が有効になっているかどうかを示します。
ステータス (Status)	イーサネット ポート 0 および 1 のポートがアップしているか、またはダウンしているかを示します。
[IPアドレス(IP Address)]	イーサネット ポート 0 の IP アドレスが表示されます(ネットワーク耐障害性(NFT)が有効な場合はイーサネット ポート 1 の IP アドレスも表示)。
IP マスク	イーサネット ポート 0 の IP マスクが表示されます(NFT が有効の場合はイーサネット ポート 1 の IP マスクも表示)。
リンク検出済み(Link Detected)	アクティブ リンクが存在するかどうかを示します。
キューの長さ(Queue Length)	キューの長さが表示されます。
MTU	最大伝送単位が表示されます。
MAC アドレス(MAC Address)	ポートのハードウェア アドレスが表示されます。
受信済み統計(RX)(Receive Statistics (RX))	受信したバイト数、パケット数、エラー数に加えて、廃棄、およびオーバーランの統計情報が表示されます。
送信済み統計(TX)(Transmit Statistics (TX))	送信したバイト数、パケット数、エラー数に加えて、廃棄、キャリア、およびコリジョンの統計情報が表示されます。
DNSの詳細(DNS Details)	
プライマリ(Primary)	プライマリ ドメイン ネーム サーバの IP アドレスが表示されます。
セカンダリ(Secondary)	セカンダリ ドメイン ネーム サーバの IP アドレスが表示されます。
Optionsosadmin-3-2	設定されている DNS オプションが表示されます。
ドメイン(Domain)	サーバのドメインが表示されます。
ゲートウェイ	イーサネット ポート 0 のネットワーク ゲートウェイの IP アドレスが表示されます。

インストールされているソフトウェア

ソフトウェア バージョンとインストールされているソフトウェア オプションを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウから [表示（Show）] > [ソフトウェア（Software）] の順に移動します。

[ソフトウェアパッケージ（Software Packages）] ウィンドウが表示されます。

ステップ 2　[ソフトウェア パッケージ（Software Packages）] ウィンドウの各フィールドについては、表 3-4を参照してください。

表 3-4　[ソフトウェアパッケージ（Software Packages）] フィールドの説明

フィールド	[説明（Description）]
パーティションのバージョン（Partition Versions）	アクティブ パーティションと非アクティブ パーティションで実行中のソフトウェアのバージョンが表示されます。
インストールされているアクティブなソフトウェア オプションのバージョン（Active Version Installed Software Options）	インストールされているソフトウェア オプションのバージョンが表示されます。アクティブ バージョンにインストールされているロケールとダイヤル プランも含まれます。
インストールされているアクティブでないソフトウェア オプションのバージョン（Inactive Version Installed Software Options）	インストールされているソフトウェア オプションのバージョンが表示されます。アクティブでないバージョンにインストールされているロケールとダイヤル プランも含まれます。

システム ステータス

システムのステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウから、[表示（Show）] > [システム（System）] に移動します。

[システム ステータス（System Status）] ウィンドウが表示されます。

ステップ 2　[システム ステータス（System Status）] ウィンドウの各フィールドについては、表 3-5を参照してください。

表 3-5　[システムステータス(System Status)] フィールドの説明

フィールド	説明
ホスト名(Host Name)	Cisco Unified Communications Operating Systemがインストールされている Cisco MCS ホストの名前が表示されます。
日付(Date)	オペレーティング システムのインストール時に指定された大陸と地域に基づいた日時が表示されます。
[タイムゾーン(Time Zone)]	インストール時に選択されたタイムゾーンが表示されます。
ロケール(Locale)	オペレーティング システムのインストール時に選択された言語が表示されます。
製品バージョン(Product Version)	オペレーティング システムのバージョンが表示されます。
プラットフォーム バージョン(Platform Version)	プラットフォームのバージョンが表示されます。
アップタイム (Uptime)	システムのアップタイム情報が表示されます。
CPU	CPU のキャパシティのうち、アイドル状態である割合、システム プロセスを実行している割合、ユーザ プロセスを実行している割合が表示されます。
メモリ	メモリの使用状況に関する情報(メモリの合計量、メモリの空き容量、メモリの使用量)がそれぞれ KB 単位で表示されます。
ディスク/アクティブ(Disk/active)	アクティブなディスクの容量の合計、空き容量、使用量が表示されます。
ディスク/非アクティブ(Disk/inactive)	非アクティブなディスクの容量の合計、空き容量、使用量が表示されます。
ディスク/ロギング(Disk/logging)	ディスク ロギング用のディスクの容量の合計、空き容量、使用量が表示されます。

IP プリファレンス

[IP 設定(IP Preferences)] ウィンドウを使用すると、システムが使用可能な登録済みポートのリストを表示できます。[IP 設定(IP Preferences)] ウィンドウには、次の情報が含まれています。

- アプリケーション
- プロトコル
- 部品番号
- タイプ(Type)
- 変換済みポート(Translated Port)
- ステータス
- [説明(Description)]

[IP 設定(IP Preferences)] ウィンドウにアクセスするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications Operating Systemの管理(Cisco Unified Communications Operating System Administration)] ウィンドウで、[表示(Show)] > [IP設定(IP Preferences)] を選択します。

[IP設定(IP Preferences)] ウィンドウが表示されます。このウィンドウには、アクティブな(以前の)クエリーのレコードも表示されることがあります。

ステップ 2　データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードをフィルタリングまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

(注)　検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア(Clear Filter)] ボタンをクリックします。

ステップ 3　[検索(Find)] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数(Rows per Page)] ドロップダウン リスト ボックスで別の値を選択します。

[IP 設定(IP Preferences)] フィールドの説明については、次を参照してください。

表 3-6　[IP 設定(IP Preferences)] フィールドの説明

フィールド	[説明(Description)]
アプリケーション	ポートを使用(リッスン)しているアプリケーションの名前。
プロトコル	このポートで使用されているプロトコル(TCP や UDP など)。
部品番号	数字のポート番号。
タイプ(Type)	このポートで許可されるトラフィックのタイプ。 • [パブリック(Public)]:すべてのトラフィックが許可される • [変換済み(Translated)]:すべてのトラフィックが許可されるが、別のポートに転送される • [非通知(Private)]:定義済みの一連のリモート サーバ(クラスタ内の他のノードなど)からのトラフィックのみ許可される

表 3-6　[IP 設定(IP Preferences)] フィールドの説明(続き)

フィールド	[説明(Description)]
変換済みポート(Translated Port)	このポートを宛先とするトラフィックは、[ポート番号(Port Number)] 列に表示されているポートに転送されます。このフィールドが適用されるのは、変換済みタイプのポートのみです。
ステータス	ポートの使用状況。 • [有効(Enabled)]:アプリケーションで使用されており、ファイアウォールで開かれている • [無効(Disabled)]:ファイアウォールでブロックされていて、未使用状態
[説明(Description)]	ポートの使用状況に関する簡単な説明。

設定

IP 設定、ホスト設定、および [ネットワークタイムプロトコル（NTP）（Netrowk Time Protocol (NTP)）] 設定の表示と変更を実行するには、[設定（Settings）] オプションを使用します。

この章は、次の項で構成されています。

- IP 設定（4-1 ページ）
- NTP サーバ（4-4 ページ）
- SMTP 設定（4-5 ページ）
- 時間設定（4-5 ページ）

IP 設定

[IP 設定（IP Settings）] オプションを使用すると、イーサネット接続の IP とポートの設定を表示および変更でき、後続ノードではパブリッシャの IP アドレスを設定できます。

ここでは、次の項目について説明します。

- イーサネット設定（4-1 ページ）
- イーサネット IPv6 の設定（4-2 ページ）
- パブリッシャ設定（4-3 ページ）

イーサネット設定

[IP 設定（IP Settings）] ウィンドウには、Dynamic Host Configuration Protocol（DHCP）がアクティブであるかどうかが表示されます。また、関連するイーサネット IP アドレスや、ネットワーク ゲートウェイの IP アドレスも表示されます。

イーサネットの設定はすべて Eth0 にのみ適用されます。Eth1 を対象とした設定はできません。Eth0 の最大伝送単位（MTU）のデフォルトは 1500 です。

IP 設定を表示するには、次の手順を実行します。

注意 Cisco Unity Connection の IP 設定を変更するには、次の手順を使用しないでください。

Connection サーバの IP アドレスを変更する方法については、http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html にある『Install and *Upgrade Guides for* Connection』の「Changing the IP Addresses of Cisco Unity Connection Servers」を参照してください。

Connection 11.x サーバのホスト名の変更については、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/11xcuciumgx.html にある『*Install, Upgrade, and Maintenance Guide for* Cisco Unity Connection 11x』を参照してください。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [IP] > [イーサネット（Ethernet）] の順に移動します。

[イーサネットの設定（Ethernet Settings）] ウィンドウの表示。[イーサネットの設定（Ethernet Settings）] ウィンドウの各フィールドの説明については、表 4-1を参照してください。

表 4-1　イーサネット設定のフィールドと説明

フィールド	説明
DHCP	DHCP が有効か無効かを示します。
ホストネーム	サーバのホスト名が表示されます。
[IPアドレス（IP Address）]	システムの IP アドレスが表示されます。
サブネット マスク（Subnet Mask）	IP サブネット マスク アドレスが表示されます。
[デフォルトゲートウェイ]	ネットワーク ゲートウェイの IP アドレスが表示されます。

イーサネット IPv6 の設定

（注）　次に示す設定は、Cisco Unity Connection リリース 9.0 以降に適用されます。IPv6 は、以前のバージョンの Cisco Unity Connection ではサポートされていません。

[イーサネットIPv6設定（Ethernet IPv6 Configuration Settings）] ページでは IPv6 を有効にし、IP アドレスを取得する方法を決定することができます。

IPv6 設定を表示または変更するには、次の手順に従います。

手順

ステップ 1　[Cisco Unified Communications Operating Systemの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定(Settings）] > [IP] > [イーサネットIPv6設定(Ethernet IPv6 Configuration）] の順に移動します。

ステップ 2　イーサネット IPv6 の設定を変更するには、適切なフィールドに新しい値を入力します。[イーサネットIPv6設定(Ethernet IPv6 Configuration Settings）] ウィンドウの各フィールドについては、表 4-2 を参照してください。

ステップ 3　変更を保存するには、[保存（Save）] を選択します。

表 4-2　[イーサネットIPv6設定(Ethernet IPv6 Configuration)] のフィールドと説明

フィールド	説明
IPv6を有効化(Enable IPv6)	IPv6 を有効にするには、このチェックボックスをオンにします。
アドレスソース(Address Source)	次のいずれかを選択します。 • [ルータアドバタイズメント(Router Advertisement)]:ネットワーク ルータがネットワーク上のサーバにネットワーク プレフィックスをアドバタイズするように設定されている場合は、このオプションを選択します。 • [DHCP]:DHCPv6 プロトコルを使用してアドレスをご自身のサーバに割り当てるにはこのオプションを選択します(アドレスを提供するためにネットワークの DHCPv6 サーバを実行する必要があることに注意してください)。 • [手動入力(Manual Entry)]:[IPv6アドレス(IPv6 Address)] フィールドにアドレスを手動で入力する場合は、このオプションを選択します。 **(注)** シスコでは、Cisco Unity Connection サーバにスタティック非リンクローカル IPv6 アドレスを使用することを推奨します。サーバが DHCPv6 サーバから、またはステートレス アドレス自動設定を介して IPv6 アドレスを取得する場合は、サーバが DHCPv6 サーバから 1 つの非リンクローカル IPv6 アドレスだけを取得することを確認してください。 **(注)** [手動入力(Manual Entry)] を指定した場合を除き、[IPv6アドレス(IPv6 Address)] および [サブネットマスク(Subnet Mask)] フィールドは読み取り専用のままです。
IPv6 アドレス(IPv6 Address)	[アドレスソース(Address Source)] として [手動入力(Manual Entry)] を選択した場合は、IPv6 アドレスを入力します。 例を示します。 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345
サブネット マスク(Subnet Mask)	[アドレスソース(Address Source)] として [手動入力(Manual Entry)] を選択した場合は、ネットワーク プレフィックスに対応するビット数を示すアドレスのプレフィックスの長さ(0 ～ 128)をアドレスに入力します。 例を示します。 64
リブートを使用した更新(Update with Reboot)	設定の更新を保存するときにサーバのリブートを即時に実行したい場合、このチェックボックスをオンにします。 **(注)** IPv6 の設定を有効にするには、システムをリブートする必要があります。

パブリッシャ設定

この機能を適用できるのは、サーバに Cisco Unified Communications Manager が単独でインストールされている場合に限られます。

NTP サーバ

外部 NTP サーバが Stratum 9 以上（1 ～ 9）であることを確認してください。外部 NTP サーバの追加、削除、または変更を行うには、次の手順に従います。

（注）　最初のノードまたはパブリッシャの NTP サーバ設定のみを設定できます。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [NTP サーバ（NTP Servers）] の順に移動します。

[NTP サーバの設定（NTP Server Settings）] ウィンドウが表示されます。

ステップ 2　NTP サーバの追加、削除、または変更ができます。

（注）　発生する可能性のある互換性の問題、精度の問題、およびネットワーク ジッターの問題を回避するには、プライマリ ノードに指定する外部 NTP サーバが NTP v4（バージョン 4）である必要があります。IPv6 アドレッシングを使用している場合は、外部 NTP サーバが NTP v4 でなければなりません。

- NTP サーバを削除するには、該当サーバの前にあるチェックボックスをオンにしてから [削除（Delete）] をクリックします。
- NTP サーバを追加するには、[追加（Add）] をクリックし、ホスト名または IP アドレスを入力してから、[保存（Save）] をクリックします。
- NTP サーバを変更するには、IP アドレスをクリックし、ホスト名または IP アドレスを変更してから、[保存（Save）] をクリックします。

（注）　NTP サーバに対する変更は、完了するまで最大で 5 分かかる場合があります。NTP サーバに変更を加える場合は、ウィンドウを更新して正しいステータスを表示する必要があります。

ステップ 3　[NTPサーバの設定（NTP Server Settings）] ウィンドウを更新して正しいステータスを表示するには、[設定（Settings）] > [NTP] の順に選択します。

（注）　NTP サーバの削除、変更、または追加後には、クラスタ内の他のすべてのノードを再起動して、変更を有効にする必要があります。

SMTP 設定

[SMTP 設定（SMTP Settings）] ウィンドウでは、SMTP ホスト名の表示や設定ができ、SMTP ホストがアクティブであるかどうかが表示されます。

ヒント　システムからの電子メール受信する場合は、SMTP ホストを設定する必要があります。

SMTP 設定にアクセスするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [SMTP] の順に移動します。

[SMTP 設定（SMTP Settings）] ウィンドウが表示されます。

ステップ 2　SMTP ホスト名または IP アドレスを入力するか、または変更します。

ステップ 3　[Save] をクリックします。

時間設定

時刻を手動で設定するには、次の手順を実行します。

（注）　サーバ時刻を手動で設定するには、設定済みの NTP サーバをすべて削除する必要があります。詳細については、「NTP サーバ」セクション（ 4-4 ページ）を参照してください。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [時間（Time）] の順に移動します。

ステップ 2　システムの日付と時刻を入力します。

ステップ 3　[保存（Save）] をクリックします。

ステップ 4　Cisco Unity Connection サーバで、日付を変更した場合、または時刻を 2 分以上変更した場合、CLI コマンド **utils system restart** でサーバを再起動します。

CHAPTER 5

システム リスタート

この項では、次の再起動オプションを使用する手順について説明します。

- バージョンの切り替えと再起動（5-1 ページ）
- 現在のバージョンの再起動（5-2 ページ）
- システムのシャットダウン（5-2 ページ）

バージョンの切り替えと再起動

このオプションは、新しいソフトウェアにアップグレードする場合と、以前のソフトウェアのバージョンにフォール バックする場合の両方で使用します。アクティブ ディスク パーティションで実行中のシステムをシャットダウンし、その後非アクティブ パーティションのソフトウェア バージョンを使用してシステムを自動的に再起動するには、次の手順に従います。

注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [バージョン（Version）] の順に移動します。

[バージョン設定（Version Settings）] ウィンドウが表示されます。このウィンドウにはアクティブ パーティションと非アクティブ パーティションの両方のソフトウェア バージョンが表示されます。

ステップ 2 バージョンを切り替えて再起動する場合は、[バージョンの切り替え（Switch Versions）] をクリックします。操作を中止する場合は、[キャンセル（Cancel）] をクリックします。

[バージョンの切り替え（Switch Versions）] をクリックするとシステムが再起動し、現在非アクティブであるパーティションがアクティブになります。

現在のバージョンの再起動

現在のパーティションでバージョンを切り替えずにシステムを再起動するには、次の手順に従います。

注意　この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [バージョン（Version）] の順に移動します。

[バージョン設定（Version Settings）] ウィンドウが表示されます。このウィンドウにはアクティブ パーティションと非アクティブ パーティションの両方のソフトウェア バージョンが表示されます。

ステップ 2　システムを再起動する場合は [リスタート（Restart）] をクリックします。操作を中止する場合は [キャンセル（Cancel）] をクリックします。

[リスタート（Restart）] をクリックすると、現在のパーティションのシステムが、バージョンを切り替えずに再起動します。

システムのシャットダウン

注意　サーバをシャットダウンおよびリブートする場合、サーバの電源ボタンを押さないでください。電源ボタンを押すと、誤ってファイル システムを破損し、サーバをリブートできなくなるおそれがあります。

システムをシャットダウンするには、手順 1 または手順 2 に従います。

注意　この手順を実行すると、システムがシャットダウンします。

手順 1

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[設定（Settings）] > [バージョン（Version）] の順に移動します。

[バージョン設定（Version Settings）] ウィンドウが表示されます。このウィンドウにはアクティブ パーティションと非アクティブ パーティションの両方のソフトウェア バージョンが表示されます。

ステップ 2　システムをシャットダウンする場合は [シャットダウン（Shutdown）] をクリックします。操作を中止する場合は [キャンセル（Cancel）] をクリックします。

[シャットダウン（Shutdown）] をクリックすると、すべてのプロセスが中断され、システムがシャットダウンします。

（注）　ハードウェアが停止するまで数分かかる場合があります。

手順 2（手順 1 の代わり）

ステップ 1　CLI コマンド **utils system shutdown** または **utils system restart** コマンドを実行します。CLI コマンドを実行する手順については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

CHAPTER 6

セキュリティ

この章では証明書の管理と IPSec の管理について説明し、次の作業を実行する手順を説明します。

- Internet Explorer のセキュリティ オプションの設定（6-1 ページ）
- 証明書と証明書信頼リストの管理（6-1 ページ）
- IPSEC の管理（6-11 ページ）

Internet Explorer のセキュリティ オプションの設定

サーバから証明書をダウンロードするには、Internet Explorer のセキュリティ設定が次のように設定されていることを確認します。

手順

ステップ 1 Internet Explorer を起動します。

ステップ 2 [ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Advanced] タブの [セキュリティ] セクションまでスクロールします。

ステップ 5 必要に応じて、[暗号化されたページをディスクに保存しない（Do not save encrypted pages to disk）] チェックボックスをオフにします。

ステップ 6 [OK] をクリックします。

証明書と証明書信頼リストの管理

次の各項では、[証明書の管理（Certificate Management）] メニューから実行できる機能を説明します。

- 証明書の表示
- 証明書のダウンロード
- 証明書の削除と再作成
- サードパーティ製の CA 証明書の使用

（注）　[セキュリティ（Security）] メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications Operating System に再ログインする必要があります。

証明書の表示

既存の証明書を表示するには、次の手順を実行します。

手順

ステップ 1　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[検索（Find）] コントロールを使用すると、証明書のリストをフィルタリングできます。

ステップ 3　証明書または信頼ストアの詳細を表示するには、[コモンネーム（Common Name）] で証明書のファイル名をクリックします。

[証明書の詳細（Certificate Details）] ウィンドウに証明書の情報が表示されます。

ステップ 4　[証明書の一覧（Certificate List）] ウィンドウに戻るには、[証明書の詳細（Certificate Details）] ウィンドウで [閉じる（Close）] をクリックします。

証明書のダウンロード

証明書を Cisco Unified Communications Operating System から PC にダウンロードするには、次の手順を実行します。

手順

ステップ 1　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[検索（Find）] コントロールを使用すると、証明書のリストをフィルタリングできます。

ステップ 3　[コモンネーム（Common Name）] で証明書のファイル名をクリックします。

[証明書の詳細（Certificate Details）] ウィンドウが表示されます。

ステップ 4　[.PEMファイルのダウンロード（Download .PEM File）] または [.DERファイルのダウンロード（Download .DER File）] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

証明書の削除と再作成

次の各項では、証明書の削除と再作成について説明します。

- 証明書の削除
- 証明書の再生成

証明書の削除

信頼できる証明書を削除するには、次の手順を実行します。

注意　証明書を削除すると、システムの動作に影響する場合があります。[証明書の一覧（Certificate List）] から選択する証明書に対する既存の CSR はシステムから削除されるので、新しい CSR を生成する必要があります。詳細については、「証明書署名要求の生成」の手順（ 6-6 ページ）を参照してください。

手順

ステップ 1　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[検索（Find）] コントロールを使用すると、証明書のリストをフィルタリングできます。

ステップ 3　[コモンネーム（Common Name）] で証明書のファイル名をクリックします。

[証明書の詳細（Certificate Details）] ウィンドウが表示されます。

ステップ 4　[Delete] をクリックします。

証明書の再生成

自己署名証明書を再作成するには、次の手順を実行します。

注意　証明書を再作成すると、システムの動作に影響する場合があります。

手順

ステップ 1　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[自己署名証明書の作成（Generate Self-signed）] または [CSRの作成（Generate CSR）] をクリックします。

[証明書の作成(Generate Certificate)] ダイアログボックスが表示されます。

ステップ 3　[証明書の名前（Certificate Name）] リストから、証明書の名前を選択します。表示される証明書の用途の説明については、表 6-1 を参照してください。

ステップ 4　[生成（Generate）] をクリックします。

（注） Cisco Unified Communications Operating System で証明書を再作成したら、バックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップの実行に関する詳細については、『*Install, Upgrade, and Maintenance Guide for Cisco Unity Connection*』を参照してください。

表 6-1　証明書の用途と説明

[名前（Name）]	説明
tomcat	この自己署名ルート証明書は、Connection サーバのインストール時に生成され、証明書タイプは RSA キーに基づきます。
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPSec 接続のインストール中に生成されます。
CallManager-ECDSA	この自己署名ルート証明書は、Connection サーバのインストール時に生成され、証明書タイプは、EC キーに基づきます。 （注） CallManager は証明書の命名規則においてのみ使用されますが、生成された証明書は Connection サーバに固有です。

サードパーティ製の CA 証明書の使用

シングルサーバとマルチサーバの証明書の概要

名前からわかるように、シングルサーバ証明書には、その FQDN のみの信頼を識別する単一の FQDN が含まれます。単一の FQDN またはドメインはサブジェクトの別名（SAN）拡張に存在します。クラスタ内に複数のサーバが存在する場合、システムは同じ数の X.509 証明書の生成を要求します。各サーバで 1 つが必要です。

システムは、複数のサーバ、あるいはドメインまたはサブドメインの信頼を識別するために、マルチサーバの証明書を使用します。マルチサーバ証明書の SAN 拡張には、複数の FQDN またはドメインが含まれます。

次の表は、シングルサーバとマルチサーバの証明書間の基本的な違いについて説明します。

表 6-2　証明書の設定の比較

シングルサーバ証明書	マルチサーバ証明書
CN フィールドおよび/または SAN 拡張子に単一の FQDN またはドメインが含まれます。	SAN 拡張子に存在する複数の FQDN またはドメインが含まれます。
システムがクラスタ内の各サーバに対して 1 つの証明書を使用します。	1 つの証明書が複数のサーバを識別します。

表 6-2　証明書の設定の比較（続き）

シングルサーバ証明書	マルチサーバ証明書
管理者は、証明書の有効期限切れ、秘密キーの侵害などの状況において各個別のサーバで証明書と秘密キーを再生成します、	この証明書はすべてのサーバに共通する 1 つの公開キーと秘密キーのペアだけをカバーするため、証明書とともにクラスタ内のすべてのサーバに対して同じ秘密キーの安全な送信が要求されます。秘密キーがサーバで侵害されたら、証明書と秘密キーはすべてのサーバに対して再生成する必要があります。
シングル サーバ証明書の生成は、クラスタの管理者にとってオーバヘッドとなる可能性があります。証明書署名要求（CSR）の生成、署名のための CSR の CA への送信、クラスタ内の各サーバの署名付き証明書のアップロードなどの手順を実行する必要があるためです。	管理者にとっては、マルチサーバ証明書を管理する上で、オーバーヘッドが少なくなります。所定のサーバで一回だけ手順を踏めばよいからです。システムは関連する秘密キーと署名付き証明書をクラスタ内のすべてのサーバに配信します。

Cisco Unified Communications Operating System は、サード パーティの認証局（CA）が PKCS # 10 証明書署名要求（CSR）を使用して発行した証明書をサポートしています。

次の表に、このプロセスの概要および参考となる文書を示します。

	タスク	詳細情報
ステップ 1	[Cisco Unified Communications オペレーティングシステムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウにログインします。	Cisco Unified Communications オペレーティング システムの管理を使用して、システム管理者はマルチサーバ オプションをサポートする個々の証明書の用途のために CSR を生成するときに、配信タイプを選択できます。システムは必要な SAN エントリを CSR に自動的に入力し、画面にデフォルトの SAN エントリを表示します。マルチサーバ CSR の生成では、システムがクラスタ内のすべての必要なサーバに自動的にその CSR を配布します。同様に、マルチサーバ CA 署名付き証明書のアップロードでは、システムがクラスタ内のすべての必要なサーバに自動的にその証明書を配布します。
ステップ 2	サーバに CSR を作成します。	「証明書署名要求の生成」セクション（6-6 ページ）
ステップ 3	CSR を PC にダウンロードします。	「証明書署名要求のダウンロード」セクション（6-7 ページ）
ステップ 4	CSR を使用して、CA からアプリケーション証明書を取得します。	アプリケーション証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「「サードパーティ製の CA 証明書」セクション（6-8 ページ）」を参照してください。
ステップ 5	CA ルート証明書を取得します。	ルート証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「「サードパーティ製の CA 証明書」セクション（6-8 ページ）」を参照してください。
ステップ 6	CA ルート証明書をサーバにアップロードします。	「信頼証明書のアップロード」セクション（6-8 ページ）

	タスク	詳細情報
ステップ 7	アプリケーション証明書をサーバにアップロードします。	「アプリケーション証明書のアップロード」セクション（6-9 ページ）
ステップ 8	新しい証明書の影響を受けるサービスを再起動します。	すべての証明書タイプで、対応するサービスを再起動します。 • Tomcat 証明書を更新する場合は、Cisco Tomcat サービス、Connection IMAP サーバ、Cisco Dirsync サービス、Connection Jetty サービス、および Connection Conversation Manager サービスを再起動する必要があります。 • CallManager ECDSA 証明書を更新する場合は、Connection Conversation Manager サービスも再起動する必要があります。 サービスの再起動の詳細については、『Cisco Unified Communications Manager *Serviceability Administration Guide*』を参照してください。

証明書署名要求の生成

証明書署名要求を再生成するには、次の手順を実行します。

手順

ステップ 1　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　証明書のリストをフィルタするには、[検索（Find）] コントロールを使用します。

ステップ 3　[CSRの作成（Generate CSR）] をクリックすると、[証明書署名要求の作成（Generate Certificate Signing Request）] ダイアログボックスが表示されます。

ステップ 4　[証明書の用途（Certificate Purpose）] ドロップダウン リスト ボックスから、必要な証明書の用途を選択します。

ステップ 5　[配布（Distribution）] ドロップダウン リスト ボックスから、必要な配布リスト項目を選択します。

（注）　マルチサーバ（SAN）オプションは、[証明書の用途（Certificate Purpose）] ドロップダウン リスト ボックスから Tomcat または CallManager-ECDSA を選択した場合にのみ使用できます。[CSR の作成（Generate CSR）] をクリックします。

（注）　デフォルトでは、システムによって CN フィールドにサーバの FQDN（またはホスト名）が読み込まれます。必要に応じて値を変更できます。自己署名証明書の場合、CN を構成できません。

ステップ 6　マルチサーバ（SAN）の場合、追加のドメインを [サブジェクト代替名（Subject Alternate Names）] フィールドに追加できます。

ステップ 7　[キーの長さ(Key Length)] ドロップダウン リスト ボックスから、証明書の用途に応じて値を選択します。
Tomcat または IPSec が証明書の用途の場合は、[1024] または [2048] を選択します。
CallManager-ECDSA が証明書の用途の場合は、[256]、[384]、または [521] を選択します。

ステップ 8　[ハッシュアルゴリズム(Hash Algorithm)] ドロップダウン リスト ボックスから、証明書の用途に応じて選択します。
Tomcat または IPSec が証明書の用途の場合は、[SHA1] または [SHA256] を選択します。
CallManager-ECDSA が証明書の用途の場合は、[SHA384 SHA512] を選択します。

ステップ 9　[生成(Generate)] をクリックして新しい CSR を生成します。

(注)　特定のタイプの証明書に対して生成される新しい CSR はそのタイプの既存の CSR を上書きします。CSR は、クラスタ内のすべての必要なサーバに自動的に配布されます。

証明書署名要求のダウンロード

証明書署名要求をダウンロードするには、次の手順を実行します。

手順

ステップ 1　[セキュリティ(Security)] > [証明書の管理(Certificate Management)] を選択します。
[証明書の一覧(Certificate List)] ウィンドウが表示されます。

ステップ 2　リストから、タイプ「CSR だけ(CSR Only)」というエントリのある共通名と、共通名に一致する配信値をクリックします。

(注)　マルチ サーバの SAN の証明書では、タイプ「CSR だけ(CSR Only)」というエントリのある共通名と、マルチサーバ(SAN)の配信値をクリックします。

[CSRの詳細(CSR Details)] ウィンドウが表示されます。

ステップ 3　[Download CSR] をクリックします。

ステップ 4　CSR のダウンロードが完了したら、[閉じる(Close)] をクリックします。

クラスタのパブリッシャとサブスクライバの両方のマルチサーバ SAN の証明書を設定した後、Tomcat サービスを再起動する必要があります。次の手順を参照してください。

手順

ステップ 1　SSH アプリケーションを使用して Unity Connection サーバにサインインします。

ステップ 2　次の CLI コマンドを使用して Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```

サードパーティ製の CA 証明書

サードパーティの CA が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と CA ルート証明書の両方を CA、またはアプリケーション証明書と CA 証明書の両方が含まれている PKCS#7 証明書チェーン（DER 形式）から取得する必要があります。これらの証明書の取得に関する情報は、CA から入手してください。入手の手順は、CA によって異なります。

Cisco Unified Communications Operating System は、PEM エンコーディング形式で CSR を生成します。システムは、DER および PEM エンコード形式の証明書と、PEM 形式の PKCS#7 証明書チェーンを受け入れます。すべての証明書タイプについて、それぞれのノードで CA ルート証明書およびアプリケーション証明書を取得してアップロードする必要があります。

Cisco Unified Communications Operating System の CSR には、CA からのアプリケーション証明書要求に含める必要がある拡張情報が含まれています。CA が拡張要求メカニズムをサポートしていない場合は、次に示すように X.509 拡張を有効にする必要があります。

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment
```

（注）　ご自身の証明書に対し証明書署名要求（CSR）を生成し、SHA256 署名によってサードパーティの CA で署名することもできます。Tomcat および他の証明書が SHA256 をサポートできるように、この署名付き証明書を Cisco Unified Communications Operating System に再度アップロードすることができます。

信頼証明書のアップロード

信頼証明書をアップロードするには、次の手順を実行します。

手順

ステップ 1　[セキュリティ（Security）] > [証明書の管理（Certificate Management）] に移動します。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2　[Upload Certificate] をクリックします。
[証明書信頼リストのアップロード（Upload Certificate Trust List）] ダイアログボックスが表示されます。

ステップ 3　[証明書の用途（Certificate Purpose）] ドロップダウンリストから、証明書を選択します。
Tomcat の信頼証明書をアップロードするには、[証明書の用途（Certificate Purpose）] リストから [Tomcatの信頼性（tomcat-trust）] を選択します。
CallManager ECDSA の信頼証明書をアップロードするには、[証明書の用途（Certificate Purpose）] リストから [CallManagerの信頼性（CallManager-trust）] を選択します。

ステップ 4　[説明（Description）] テキスト ボックスに、CA ルート証明書の名前を入力します。

ステップ 5　アップロードするファイルを選択し、[参照（Browse）] ボタンをクリックしてファイルに移動し、[開く（Open）] をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、[ファイルのアップロード（Upload File）] ボタンをクリックします。

（注）　信頼証明書の場合、システムはクラスタの他のノードに証明書を自動的に配布します。

アプリケーション証明書のアップロード

Cisco Unified Communications オペレーティング システムは、PKCS#10 証明書署名要求（CSR）を使用してサードパーティの CA が発行する証明書をサポートしています。

手順

ステップ 1　サーバに CSR を作成します。

ステップ 2　CSR を PC にダウンロードします。

ステップ 3　CSR を使用して、CA または PKCS#7 形式の証明書チェーン（CA 証明書に加えてアプリケーション証明書が含まれている場合があります）からアプリケーション証明書を取得します。

ステップ 4　CA 証明書または証明書チェーンを取得します。
Tomcat のアプリケーション証明書をアップロードするには、[証明書の用途（Certificate Purpose）] リストから [Tomcat] を選択します。
IPSec アプリケーション証明書をアップロードするには、[証明書の用途（Certificate Purpose）] リストから [IPsec] を選択します。
CallManager-ECDSA アプリケーション証明書をアップロードするには、[証明書の用途（Certificate Purpose）] リストから [CallManager-ECDSA] を選択します。

ステップ 5　アップロードするファイルを選択し、[参照（Browse）] ボタンをクリックしてファイルに移動し、[開く（Open）] をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、[ファイルのアップロード（Upload File）] ボタンをクリックします。

（注）　システムはアプリケーション証明書を他のクラスタ ノードに自動的に配布しません。複数のノードで同じ証明書が必要な場合は、証明書を各ノードに個別にアップロードする必要があります。一方、SAN 証明書の場合は、システムは他のクラスタ ノードに証明書を自動的に配布します。

証明書の有効期限日のモニタ

証明書の有効期限日が近づいたときに、システムから自動的に電子メールを送信できます。証明書有効期限モニタの表示と設定をするには、次の手順を実行します。

手順

ステップ 1　現在の**証明書有効期限モニタ**の設定を表示するには、[セキュリティ（Security）] > [証明書モニタ（Certificate Monitor）] を選択します。

[証明書モニタ（Certificate Monitor）] ウィンドウが表示されます。

ステップ 2　必要な設定情報を入力します。**証明書モニタの有効期限**のフィールドの説明については、表 6-3 を参照してください。

ステップ 3　変更を保存するには、[保存（Save）] をクリックします。

表 6-3　[証明書モニタ(Certificate Monitor)] フィールドの説明

フィールド	説明
通知開始時期(Notification Start Time)	証明書が無効になる何日前に通知を送信してもらうかを入力します。
通知の頻度(Notification Frequency)	通知の頻度を時間または日単位で入力します。
メール通知の有効化(Enable E-mail Notification)	電子メール通知を有効にするには、このチェックボックスをオンにします。
電子メール ID(Email IDs)	通知の送信先電子メール アドレスを入力します。 **(注)** システムから通知を送信するには、SMTP ホストを設定する必要があります。

証明書の失効

次の項では、[証明書失効(Certificate Revocation)] メニューから実行できる機能を説明します。

オンライン証明書ステータス プロトコルの設定

オンライン証明書ステータス プロトコル（OCSP）を使用して、証明書の失効ステータスを取得できます。OCSP を設定するには、次の手順を実行します。

手順

ステップ 1　[セキュリティ(Security)] > [証明書失効(Certificate Revocation)] に移動します。[証明書失効(Certificate Revocation)] ウィンドウが表示されます。

ステップ 2　[オンライン証明書ステータスプロトコルの設定(Online Certificate Status Protocol Configuration)] 領域で [OCSPの有効化(Enable OCSP)] チェックボックスをオンにします。

ステップ 3　証明書が OCSP URI を使用して設定されていて、OCSP レスポンダに連絡するために使用される場合は、[証明書のOCSP URIを使用(Use OCSP URI from Certificate)] を選択します。

ステップ 4　外部または設定済みの URI が OCSP レスポンダに連絡するために使用される場合は、[設定済みのOCSP URIを使用(Use configured OCSP URI)] を選択します。[OCSPの設定済みURI(OCSP Configured URI)] フィールドに、証明書失効ステータスが確認されている、OCSP レスポンダの URI を入力します。

ステップ 5　失効チェックを実行するために [失効チェックの有効化(Enable Revocation Check)] チェックボックスをオンにします。

(注)　証明書失効サービスは、失効と有効期限のチェックのエンタープライズ パラメータが有効に設定されている場合、LDAP および IPSec 接続に対してアクティブです。

ステップ 6　証明書失効ステータスの周期を確認するには、[チェック間隔(Check Every)] の値を入力します。

- 失効ステータスを毎時間ごとまたは毎日確認するには、[時間(Hours)] または [日(Days)] をクリックします。

ステップ 7　[保存(Save)] をクリックします。

警告　**OCSP を有効にする前に、tomcat-trust に OCSP レスポンダ証明書をアップロードする必要があります。**

(注)
- 証明書失効ステータス チェックは、証明書または証明書チェーンのアップロード時にのみ実行されます。証明書が失効している場合、適切なアラームが表示されます。
- Cisco Certificate Expiry Monitor サービスは、証明書失効を確実にするために再起動する必要があります。[Cisco Unifiedサービスアビリティ(Cisco Unified Serviceability)] > [ツール(Tool)] > [コントロールセンタ-ネットワークサービス(Control Center - Network Services)] に移動し、**Cisco Certificate Expiry Monitor** サービスを再起動します。

IPSEC の管理

次の各項では、[IPSec] のメニューで実行できる機能を説明します。

- 新しい IPSec ポリシーの設定
- 既存の IPSec ポリシーの管理

(注)　IPSec は、インストール時にクラスタ内のノード間で自動的に設定されません。

新しい IPSec ポリシーの設定

新しい IPSec ポリシーとアソシエーションを設定するには、次の手順を実行します。

(注)　システムのアップグレード中に IPSec ポリシーに何らかの変更を行ってもその変更は無効になるので、アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意　IPSec はシステムのパフォーマンスに影響します(特に暗号化した場合)。

手順

ステップ 1　[セキュリティ(Security)] > [IPSEC 設定(IPSEC Configuration)] を選択します。

[IPSECポリシーの一覧(IPSEC Policy List)] ウィンドウが表示されます。

ステップ 2　[新規追加(Add New)] をクリックします。

[IPSECポリシーの設定(IPSEC Policy Configuration)] ウィンドウが表示されます。

ステップ 3　[IPSECポリシーの設定(IPSEC Policy Configuration)] ウィンドウに適切な情報を入力します。このウィンドウの各フィールドの説明については、表 6-4 を参照してください。

ステップ 4　新しい IPSec ポリシーを設定するには、[保存(Save)] をクリックします。

表 6-4　[IPSECポリシーとアソシエーション(IPSEC Policy and Association)] フィールドの説明

フィールド	説明
ポリシー グループ名(Policy Group Name)	IPSec ポリシー グループの名前を指定します。名前には、文字、数字、ハイフンのみを使用できます。
ポリシー名	IPSec ポリシーの名前を指定します。名前には、文字、数字、ハイフンのみを使用できます。
認証方式(Authentication Method)	認証方式を指定します。
事前共有キー(Preshared Key)	[認証方式(Authentication Method)] フィールドで [事前共有キー(Pre-Shared Key)] を選択した場合は、事前共有キーを指定します。 **(注)** 事前共有 IPSec キーには、英字およびハイフンのみ使用できます。空白文字またはその他の文字は使用できません。Windows ベース バージョンの Cisco Unified Communications Manager から移行する場合、現行バージョンの Cisco Unified Communications Manager と互換性があるように事前共有 IPSec キーの名前を変更する必要があります。
ピア タイプ(Peer Type)	ピアのタイプが同じか異なるかを指定します。
[宛先アドレス(Destination Address)]	接続先の IP アドレスまたは FQDN を指定します。
[接続先ポート(Destination Port)]	接続先のポート番号を指定します。
ソース アドレス(Source Address)	ソースの IP アドレスまたは FQDN を指定します。
送信元ポート	ソースのポート番号を指定します。
[モード(Mode)]	転送モードを指定します。
リモート ポート(Remote Port)	接続先で使用されるポート番号を指定します。
プロトコル	次のプロトコルまたは Any を指定します。 • [TCP] • UDP • 任意(Any)
暗号化アルゴリズム(Encryption Algorithm)	ドロップダウンリストから、暗号化アルゴリズムを選択します。選択肢は次のとおりです。 • DES • 3DES
ハッシュ アルゴリズム(Hash Algorithm)	ハッシュ アルゴリズムを指定します。 • SHA1:フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム • MD5:フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム

表 6-4　[IPSECポリシーとアソシエーション(IPSEC Policy and Association)] フィールドの説明(続き)

フィールド	説明
ESP アルゴリズム(ESP Algorithm)	ドロップダウンリストから、ESP アルゴリズムを選択します。選択肢は次のとおりです。 • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
フェーズ 1 のライフタイム(Phase One Life Time)	フェーズ 1 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
フェーズ 1 の DH(Phase One DH)	ドロップダウンリストから、フェーズ 1 の DH 値を選択します。2、1 および 5 から選択できます。
フェーズ 2 のライフタイム(Phase Two Life Time)	フェーズ 2 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
フェーズ 2 の DH(Phase Two DH)	ドロップダウンリストから、フェーズ 2 の DH 値を選択します。2、1 および 5 から選択できます。
ポリシーを有効(Enable Policy)	ポリシーを有効にするには、このチェックボックスをオンにします。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、イネーブル/ディセーブル、または削除するには、次の手順を実行します。

(注) システムのアップグレード中に IPSec ポリシーに何らかの変更を行ってもその変更は無効になるので、アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意 IPSec はシステムのパフォーマンスに影響します(特に暗号化した場合)。

注意 既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

手順

ステップ 1　[セキュリティ(Security)] > [IPSEC 設定(IPSEC Configuration)] を選択します。

(注) [セキュリティ(Security)] メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications Operating System に再ログインする必要があります。

[IPSECポリシーの一覧(IPSEC Policy List)] ウィンドウが表示されます。

ステップ 2　ポリシーを表示、有効、または無効にするには、次の手順を実行します。

a. ポリシー名をクリックします。

[IPSECポリシーの設定(IPSEC Policy Configuration)] ウィンドウが表示されます。

b. ポリシーをイネーブルまたはディセーブルにするには、[ポリシーの有効化(Enable Policy)] チェックボックスを使用します。

c. [保存(Save)] をクリックします。

ステップ 3　1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a. 削除するポリシーの横にあるチェックボックスをオンにします。

[すべてを選択(Select All)] をクリックするとすべてのポリシーを選択でき、[すべてをクリア(Clear All)] を選択するとすべてのチェックボックスをクリアできます。

b. [Delete Selected] をクリックします。

CHAPTER 7

ソフトウェアのアップグレード

カスタム ログイン メッセージの設定

カスタマイズされたログイン メッセージをアップロードするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[ソフトウェア アップグレード（Software Upgrades）] > [ログイン メッセージのカスタマイズ（Customized Logon Message）] を選択します。

[ログインメッセージのカスタマイズ（Customized Logon Message）] ウィンドウが表示されます。

ステップ 2 アップロードするテキスト ファイルを選択するには、[参照（Browse）] をクリックします。

ステップ 3 [ファイルのアップロード（Upload File）] をクリックします。

（注） アップロードできるファイルは 10 KB 以内です。

システムにカスタマイズされたログイン メッセージが表示されます。

ステップ 4 デフォルトのログイン メッセージに戻すには、[削除（Delete）] をクリックします。

カスタマイズされたログイン メッセージが削除され、システムにデフォルトのログイン メッセージが表示されます。

サービス

この章では、他のシステムに対する ping やリモート サポートの設定など、このオペレーティング システムで使用可能なユーティリティ機能について説明します。

この章は、次の項で構成されています。

- ping（8-1 ページ）
- リモート サポート（8-2 ページ）

ping

[pingユーティリティ（Ping Utility）] ウィンドウでは、ネットワーク内の別のサーバに ping を送信できます。

別のシステムに ping を送信するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、[サービス（Services）] > [Ping] の順に移動します。

[リモートのping（Ping Remote）] ウィンドウが表示されます。

ステップ 2 ping の送信先となるシステムの IP アドレスまたはネットワーク名を入力します。

ステップ 3 ping 間隔を秒単位で入力します。

ステップ 4 パケット サイズを入力します。

ステップ 5 ping 回数（システムに ping を送信する回数）を入力します。

（注） 複数回の ping を指定した場合は、ping コマンドを入力してもリアルタイムでは ping の日時が表示されません。**ping** コマンドがデータを表示するのは、指定した回数だけ ping を送信した後です。

ステップ 6 IPSec を検証するかどうかを選択します。

ステップ 7 [Ping] をクリックします。

[リモートのping（Ping Remote）] ウィンドウに ping の統計情報が表示されます。

リモート サポート

[リモートアカウントのサポート(Remote Account Support)] ウィンドウで、シスコのサポート担当者が指定日時にシステムにアクセスできるようにするためのリモート アカウントを設定できます。

リモート サポートは次の手順で行われます。

1. ユーザがリモート サポート アカウントを設定します。このアカウントには、シスコの担当者がアクセスできる制限時間があります。この制限時間は、さまざまな値に設定できます。
2. リモート サポート アカウントを設定すると、パス フレーズが生成されます。
3. ユーザはシスコのサポートに電話し、リモート サポート アカウント名とパス フレーズを伝えます。
4. シスコのサポート担当者はパスフレーズをデコーダ プログラムに入力し、パス フレーズからパスワードを生成します。
5. シスコのサポート担当者は、デコードしたパスワードを使用して、お客様のシステム上のリモート サポート アカウントにログインします。
6. アカウントの制限時間が経過すると、シスコのサポート担当者はリモート サポート アカウントにアクセスできなくなります。

リモート サポートを設定するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications オペレーティング システムの管理(Cisco Unified Communications Operating System Administration)] ウィンドウで、[サービス(Services)] > [リモート サポート(Remote Support)] の順に移動します。

[リモートアクセスの設定(Remote Access Configuration)] ウィンドウが表示されます。

ステップ 2　[アカウント名(Account Name)] フィールドにリモート アカウントのアカウント名を入力します。

アカウント名は 6 文字以上にする必要があり、すべてアルファベットの小文字を使用します。

ステップ 3　[アカウントの有効期限(Account Duration)] フィールドにアカウントの有効期間を日数で入力します。

デフォルトのアカウントの有効期限は 30 日です。

ステップ 4　[Save] をクリックします。

[リモートサポートのステータス(Remote Support Status)] ウィンドウが表示されます。[リモートサポートのステータス(Remote Support Status)] ウィンドウの各フィールドについては、表 8-1 を参照してください。

ステップ 5　生成されたパス フレーズを使用してシステムにアクセスする方法については、シスコの担当者にお問い合わせください。

ステップ 6　リモート アクセス サポート アカウントを削除するには、[削除(Delete)] ボタンをクリックします。

表 8-1　[リモート サポートのステータス(Remote Support Status)] のフィールドと説明

フィールド	説明
デコード バージョン(Decode version)	使用中のデコーダのバージョンが示されます。
アカウント名(Account name)	リモート サポート アカウントの名前が表示されます。
有効期限(Expiration)	リモート アカウントへのアクセスが期限切れになる日時が表示されます。
パス フレーズ(Pass phrase)	生成されたパス フレーズが表示されます。

INDEX

I

IPSec
- 新しいポリシーの設定 6-11
- ポリシー フィールド（表） 6-12
- ポリシーの表示 6-13
- ポリシーの変更 6-13

N

NTP サーバ設定 4-4

い

インストールされているソフトウェア
- 手順 3-4
- フィールド（表） 3-4

お

オペレーティング システム
- ネットワーク ステータス フィールド（表） 3-3
- ハードウェア ステータス
  - 手順 3-2
  - フィールド（表） 3-2
- はじめに 1-1
- ログイン 2-1

く

クラスタ ノード
- フィールド（表） 3-1

さ

サービス
- リモート サポート
  - 概要 8-2
  - 設定 8-2

し

システム
- シャットダウン 5-2
- ステータス
  - 手順 3-4
  - フィールド（表） 3-5

シャットダウン、オペレーティング システム 5-2

証明書
- 再作成 6-3
- 削除 6-3
- ダウンロード 6-2
- 表示 6-2
- 有効期限モニタ フィールド（表） 6-10

す

ステータス
- システム
  - 手順 3-4
  - フィールド（表） 3-5
- ネットワーク
  - フィールド（表） 3-3
- ハードウェア
  - 手順 3-2
  - フィールド（表） 3-2

せ

設定
IP 4-1
NTP サーバ 4-4
イーサネット
フィールド（表） 4-2

そ

ソフトウェア
インストール済み
手順 3-4
フィールド（表） 3-4

ね

ネットワーク ステータス
フィールド（表） 3-3

の

ノード、クラスタ
フィールド（表） 3-1

は

ハードウェア、ステータス
手順 3-2
フィールド（表） 3-2

り

リモート サポート 8-2
ステータス フィールド（表） 8-3
設定 8-2

ろ

ログイン
概要 2-1